UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, v. JAMES GATTO, a/k/a "Jim," MERL CODE, and CHRISTIAN DAWKINS, Defendants.	:	Case No. 17-cr-00686 (LAK)

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION TO SUPPRESS EVIDENCE OBTAINED FROM THE SEARCH OF DEFENDANTS' CELL PHONES

NEXSEN PRUET LLC
William W. Wilkins
Mark C. Moore
Andrew A. Mathias
55 E. Camperdown Way, Suite 400
Greenville, South Carolina 29601
(864) 370-2211

Attorneys for Defendant Merl Code

HANEY LAW GROUP PLLC
Steven A. Haney
3000 Town Center Drive, Suite 2570
Southfield, Michigan 48075
(248) 414-1470

Attorneys for Defendant Christian Dawkins

WILLKIE FARR & GALLAGHER LLP
Michael S. Schachter
Casey E. Donnelly
787 Seventh Avenue
New York, New York 10019
(212) 728-8000

ANGELI LAW GROUP LLC
David Angeli
121 SW Morrison Street, Suite 400
Portland, Oregon 97204
(503) 222-1552

Attorneys for Defendant James Gatto

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Case **Page(s)**

Statutes

Other Authorities

Defendants James Gatto, Merl Code and Christian Dawkins respectfully submit this memorandum of law in support of their motion to suppress all evidence seized pursuant to the search of their cell phones.

PRELIMINARY STATEMENT

Cell phones are much more than devices used to make phone calls: they are portable computers, capable of storing an ever-increasing amount of deeply personal data. People are seldom far from their cell phones, and the devices chronicle every aspect of a person's existence. Cell phones track every website that the owner visited. They can record exactly where the owner was on a particular day, and for how long. They store intimate photographs and videos that the owner has taken. They contain a record of the owner's private communications. In short, a cell phone is a window into its owner's entire life.

Based on evidence that Mr. Gatto used his cell phone for eight calls, evidence that Mr. Code used his phone for thirteen calls, and evidence that Mr. Dawkins used his phone for calls and a single text message, the Government obtained warrants to search the *entirety* of the data contained on Defendants' phones—including photos, videos, internet search history, applications, emails, calendars, and other matter. The fact that the phones were used for calls, however, does not create probable cause to believe that evidence of criminality would be found within the electronic data contained on the phones. It goes without saying that the content of phone calls does not reside on the phones used to make those calls. But other than these calls, and, with respect to Mr. Dawkins, a single text message, the Government's search warrant applications presented no evidence that the *data* on Defendants' phones contained incriminating evidence. The few communications identified in the warrant applications do not provide probable cause to believe evidence of a crime may be found on Defendants' phones—and do not support the all-encompassing sweep of electronic data contained therein that the warrants

authorized. Any evidence seized from the searches of Defendants' phones should therefore be suppressed and the Government should immediately return Defendants' cell phones, as well as the imaged copies of the cell phone data it maintains, to Defendants.

FACTUAL BACKGROUND

Following Defendants' arrests, the Government submitted applications for warrants to search their phones (the "Warrant Applications" or "Applications"). (*See* Ex. 1 (Gatto Application); Ex. 2 (Code Application); Ex. 3 (Dawkins Application).) The warrants were issued on the same day the applications were submitted (the "Search Warrants" or "Warrants"). (*See* Ex. 4 (Gatto Warrant); Ex. 5 (Code Warrant); Ex. 6 (Dawkins Warrant).)

A. The Government's Warrant Applications.

Each of the Warrant Applications described evidence of the scheme alleged in the Complaint and Indictment, but provided virtually no connection between this alleged misconduct and the electronic data stored on Defendants' phones. With respect to Mr. Gatto, the Government's Application purports to establish probable cause sufficient to seize and search his cell phone based only on evidence of eight phone calls made with Mr. Gatto's iPhone—the content of which, of course, would not reside on his phone. (Ex. 1 at JG_00000009-10.)

With respect to Mr. Code, the Warrant Application references a total of thirteen calls—recorded over a span of three months—in which Mr. Code participated via his BlackBerry Passport phone. (Ex. 2 at MC_00000011-17.) The Application also states that during one of these calls, Mr. Dawkins informed Mr. Code that he would text Mr. Code a list of coaches Mr. Code could introduce to UC-1. (*Id*. at MC_00000014, ¶17(b).) With respect to Mr. Code's Kyocera phone, the Application identifies one intercepted call in which Mr. Code and Mr. Dawkins purportedly discussed payments in furtherance of the charged offenses, and notes that

Mr. Code was in possession of the Kyocera phone when he was arrested. (*Id*. at MC_00000016, ¶20.)

Finally, with respect to Mr. Dawkins, the Warrant Application cites a total of twenty calls and one text message, intercepted over a period of four months, tied to Mr. Dawkins's black iPhone. (Ex. 3 at CD_00000083-84.) With respect to Mr. Dawkins's white iPhone, the Application references an intercepted call between Mr. Dawkins and Mr. Code "using a second cellular phone number," and notes that Mr. Dawkins was carrying the white iPhone on his way to a meeting with an undercover agent when he was arrested. (*Id.* at CD_00000084 ¶18.)

Beyond references to the use of these phones for calls (one of which indicated Mr. Dawkins would text Mr. Code) and a single intercepted text message, the Warrant Applications provide no basis to conclude that evidence of criminality would be found in the emails, internet search history, notes, photos, videos, or in any of the other data contained on Defendants' phones. To fill that void, the authoring FBI agent asserts in the Applications with respect to Messrs. Gatto and Code that, based on his "training and [approximately one and a half years of] experience," he "is aware that cell phones like the Subject Device that have been used to communicate with others about fraud schemes, often contain records of that activity, including call logs, voicemail messages, text messages, email correspondence, contact information and other identifying data regarding co-conspirators, notes about calls and meetings relevant to the Subject Offenses, and the like." (Ex. 1 at JG_00000010, ¶¶1, 12); Ex. 2 at MC_00000016, ¶1, 21.) The Dawkins Application offers the more limited—but entirely generic—observation that cell phones "can be used to make and receive telephone calls, and send and receive text messages and emails." (Ex. 3 at CD_00000081, ¶6.)

B. The Authorizations In The Warrants.

The Gatto and Code Warrants authorize the search of their cell phones for, among other things, "evidence of, including communications regarding, the provision of any payments, goods, services, and/or favors" to a multitude of individuals and entities. (Ex. 4 at JG_00000047, Item II(a)-(c), (e); Ex. 5 at MC_00000020, Item II(c).) Among other things, the Dawkins Warrant authorizes the search of Mr. Dawkins's cell phones for "[e]vidence of, including communications regarding, payments to high school or college athletes." (Ex. 6 at CD_00000183, Item II(c).)

To find this evidence, the Search Warrants authorize law enforcement to search the *entirety* of the data contained on Defendants' phones:

> This warrant authorizes the seizure of the Subject Device as well as the copying of electronically stored information ["ESI"] on the Subject Device for later review . . . . In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. *Such techniques may include, but shall not be limited to, surveying various file directories or folders and the individual files they contain; conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas* to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

(Ex. 4 at JG_00000048; Ex. 5 at MC_00000115; Ex. 6 at CD_00000184.) (emphasis added).) The Warrants state that "*a complete review of the seized ESI may require examination of all of the seized data* to evaluate its contents and determine whether the data is responsive to the warrant." (*Id*. (emphasis added).)

LEGAL STANDARD

The Fourth Amendment mandates that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The "specific evil" that the Fourth Amendment aims to combat "is the 'general warrant' abhorred by the colonists[.]" *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S. Ct. 2022, 2038 (1971). To that end, the Fourth Amendment protects against "wide-ranging exploratory searches" unsupported by probable cause. *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S. Ct. 1013, 1016 (1987).

Given the nature and concentration of deeply personal information that people store on computers, cell phones, and other forms of electronic devices, the Second Circuit has recognized that the Fourth Amendment's privacy protections are particularly important in connection with the searches of electronic data. The Circuit has explained that "advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain," and that "[t]here is, thus, a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013) (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (quotation marks omitted)); *see also United States v. Ganias*, 755 F.3d 125, 134-35 (2d Cir. 2014) *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016) ("The[] Fourth Amendment protections apply to modern computer files. Like 18th Century 'papers,' computer files may contain intimate details

regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted.").

The Supreme Court shares the Second Circuit's concerns. It has emphasized the potential for privacy invasion inherent in searches of cell phones. In particular, the Court has noted that "a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," and that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]" *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

"[A] warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459, 131 S. Ct. 1849, 1856 (2011). In addition to ensuring that there is probable cause to seize and search a cell phone, courts must also give special attention to whether a warrant to search a cell phone is impermissibly overbroad. A search warrant is overbroad in violation of the Fourth Amendment if its "description of the objects to be seized is . . . broader than can be justified by the probable cause upon which the warrant is based." *Galpin*, 720 F.3d at 446; *see also United States v. Hernandez*, No. 09CR625(HB), 2010 WL 26544, at *8 (S.D.N.Y. Jan. 6, 2010) (courts must focus on whether probable cause exists "to support the breadth of the search that was authorized.") (*quoting United States v. Dinero Express, Inc.,* 99-CR-975, 2000 WL 254012, at *9 (S.D.N.Y. Mar. 6, 2010) (quotation marks omitted)); *see also United States v. Cioffi*, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009) ("Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based.") (quoting *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (quotation marks omitted)). A warrant that purports to

"authorize the seizure of, essentially, all documents" from a property exceeds the scope of probable cause. *United States v. Wey*, 256 F. Supp. 3d 355, 393 (S.D.N.Y. 2017).

In the context of searches of electronic data, the Government is permitted to "mirror" or copy the data to execute the search. *United States v. Ganias*, 824 F.3d 199, 215 (2d Cir. 2016); *see also* Fed. R. Crim. Pro. 41(e)(2)(B) (a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information" and may "authorize[] a later review of the media or information consistent with the warrant."). But the scope of the search of any copied or imaged data must be limited by the probable cause underlying the search warrant. *Galpin*, 720 F.3d at 453 (suppressing evidence obtained from an electronic search when the search went "beyond the scope" of the probable cause).

Evidence obtained in violation of the Fourth Amendment must be excluded. *Herring v. United States*, 555 U.S. 135, 139, 129 S. Ct. 695, 699 (2009). Suppression is the appropriate remedy where the affidavit submitted in support of a search warrant is "'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" *United States v. Leon*, 468 U.S. 897, 923, 104 S. Ct. 3405, 3421 (1984) (*quoting Brown v. Illinois*, 422 U.S. 590, 609, 95 S. Ct. 2265 (1984)). Additionally, "a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid," and evidence obtained from a search pursuant to such a warrant must be suppressed. *Leon*, 468 U.S. at 923. 104 S. Ct. at 3421 (1984); *see also United States v. Rosa*, 634 F.3d 639, 641 (2d Cir. 2011) (Kaplan, J., dissenting) ("exclusion is appropriate where, as here, a reasonable officer could not have presumed the warrant to have been valid."). "The burden is on the government to demonstrate the objective

reasonableness of the officers' good faith reliance" on an invalidated warrant. *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992).

ARGUMENT

I. THE WARRANTS DO NOT ESTABLISH PROBABLE CAUSE TO SEIZE AND SEARCH DEFENDANTS' CELL PHONES.

A search warrant application purporting to establish that an individual has engaged in criminal activity does not provide probable cause to search the entirety of that individual's possessions. *See United States v. Pabon*, 871 F.3d 164, 181 (2d Cir. 2017) ("[A] determination of probable cause to search is not the same as a determination that there is, at the same time, probable cause to arrest, or vice versa."); *United States v. Burton*, 288 F.3d 91, 103 (3d Cir. 2002) ("[P]robable cause to arrest does not automatically provide probable cause to search the arrestee's home."); *United States v. Santarsiero*, 566 F. Supp. 536, 538 (S.D.N.Y. 1983) ("Probable cause to arrest an individual does not, in and of itself, provide probable cause to search that person's home or car."). Rather, the probable cause must be based on "a sufficient nexus between the criminal activities alleged" and the location or items searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004). In particular, searches must be supported by probable cause showing that there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332 (1983).

Here, the Government did not provide a sound basis to conclude that Defendants' cell phones would contain evidence of wrongdoing. The only nexus identified between Mr. Gatto's phone and his alleged criminality is that he used the phone for eight calls. The Gatto Application does not suggest that he communicated via text message or that he otherwise used his phone in any way, other than those eight calls. The content of those calls does not reside on

Mr. Gatto's phone. The assertion that Mr. Gatto may be engaged in alleged criminal activity as a general matter does not give the Government license to rummage through the data stored on his phone. *See, e.g.*, *United States v. Moran*, 349 F. Supp. 2d 425, 476 (N.D.N.Y. 2005) (evidence of multiple calls between defendant and a drug trafficking co-conspirator is an "insufficient basis for finding probable cause to search [defendant's] residence.").

The same is equally true for Mr. Code and Mr. Dawkins. With the exception of a single intercepted text message in the case of Mr. Dawkins, and a reference to a text message on a phone call in the case of Mr. Code, the Applications to search their phones fail to set forth any nexus between their alleged misconduct and the data stored on their phones. Nor can probable cause be found in the FBI agent's bare assertion that cell phones that have been used to communicate with others about fraud schemes "often contain records of that activity, including call logs, voicemail messages, text messages, email correspondence, contact information and other identifying data regarding co-conspirators, notes about calls and meetings relevant to the [charged offenses], and the like." (Ex. 1 at JG_00000010, ¶12); Ex. 2 at MC_00000016, ¶21.); *see, e.g, United States v. Rutherford*, 71 F. Supp. 3d 386, 392 (S.D.N.Y. 2014) ("a conclusory legal allegation is insufficient to establish the existence of probable cause sufficient to support the issuance of a search warrant."); *United States v. Kortright*, No. 10 Cr. 937(KMW), 2011 WL 4406352, at *7 (S.D.N.Y. Sept. 13, 2011) (finding no probable cause to search defendant's residence based on the agent's opinion that it is common for drug traffickers to store contraband at their residence); *United States v. Guzman*, No. S5 97 CR 786(SAS), 1998 WL 61850, at *4 (S.D.N.Y. Feb. 13, 1998) ("Permitting 'a search warrant based solely on the self-avowed expertise of a law-enforcement agent, without any other factual nexus to the subject property, would be an open invitation to vague warrants authorizing virtually automatic searches of any

property used by a criminal suspect.'") (quoting *United States v. Rosario*, 918 F. Supp. 524, 531 (D.R.I. 1996)).

Permitting a search of all of the data stored on Defendants' cell phones based on the fact that they used them to make phone calls is no different than permitting the Government to search the photo albums and videotapes found in a person's home simply because that person made phone calls from his landline. In fact, searching an individual's cell phone is an even *greater* invasion of his privacy than is searching his home. As the Supreme Court explained, "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 134 S. Ct. at 2491.

Because the facts set forth in the Warrant Applications do not establish probable cause to seize and search Defendants' cell phones, evidence obtained as a result of these searches must be suppressed.

II. THE WARRANTS ARE OVERBROAD BECAUSE THEY DO NOT LIMIT THE SCOPE OF THE SEARCHES TO THE LOCATIONS OF DATA FOR WHICH THERE EXISTS PROBABLE CAUSE TO SEARCH.

Evidence from Defendants' cell phones must also be suppressed because the Search Warrants were overbroad. Based on evidence that the phones were used for some number of calls, one of which referenced a text message,[1] and in the case of Mr. Dawkins, a single text message, the Warrants permitted a search of all the electronic data on the phones. The Warrants in no way limited the scope of the authorized search to the locations of electronic data on the phone for which there would be probable cause to believe evidence of a crime may

[1] None of Mr. Gatto's calls referenced a text message. According to the Code Application, Mr. Dawkins said he would send a text message to Mr. Code. (Ex. 2 at MC_00000014, ¶17(b).)

be found. *Garrison*, 480 U.S. at 84, 107 S. Ct. at 1016 ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [Fourth Amendment] ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.")

The Warrants authorized "*examination of all of the seized data* to evaluate its contents and determine whether the data is responsive to the warrant." (Ex. 4 at JG_00000048; Ex. 5 at MC_00000115; Ex. 6 at CD_00000184) (emphasis added). In performing this examination, law enforcement was authorized to "conduct[] a *file-by-file* review by 'opening' or reading the first few 'pages' of such files" and "perform[] electronic 'key-word' searches through *all electronic storage areas*[.]" (*Id*. (emphasis added).)

The allegations in the Warrant Applications do not support the all-encompassing sweep of electronically stored information that the Warrants authorized. *See United States v. Juarez*, No. 12 CR 59 (RRM), 2013 WL 357570, at *3 (E.D.N.Y. Jan. 29, 2013) (Second Circuit precedent "guards against a general search of all of [a cell phone's] records, files and data."); *United States v. Vilar*, No. S305 Cr. 621, 2007 WL 1075041, at *20 (S.D.N.Y. Apr. 4, 2007) (probable cause to search certain offices for certain documents did not support the broad seizure of *all* business records).

Several decisions are particularly instructive here. In *United States v. Winn*, which District Judge Alison J. Nathan recently cited with approval, the defendant was alleged to have used his cell phone to photograph or videotape a group of teenage girls in their swimsuits without permission. 79 F. Supp. 3d 904, 909 (S.D. Ill. 2015); *see Wey*, 256 F. Supp. 3d at 392 (citing *Winn*). Law enforcement confiscated the defendant's phone and applied for a warrant to

search it nine days later. *Winn*, 79 F. Supp. 3d at 910-11. The application, which was approved by the reviewing Judge, listed a number of items to be seized from the phone, including "any or all files contained on said cell phone and its SIM Card or SD Card[.]" *Id*. at 911. The defendant moved to suppress the evidence obtained from his cell phone, arguing that the search warrant was impermissibly overbroad. *Id*. at 912. The district court agreed, noting that although there was probable cause to believe that *photos* and *videos* on the defendant's phone would contain evidence of public indecency, nothing in the search warrant application offered any basis to believe that the calendar, phonebook, contacts, SMS messages, MMS messages, emails, ringtones, audio files, call logs, installed application data, GPS information, WIFI information, internet history and usage, or system files were connected with the defendant's alleged crime. *Id*. at 919-20. As the court explained, the warrant application:

> establishe[d] that the police had probable cause to look for and seize a very small and specific subset of data on [the defendant's] cell phone. *But the warrant did not limit the scope of the seizure to only that data or describe that data with as much particularity as the circumstances allowed. Instead, the warrant contained an unabridged template that authorized the police to seize the entirety of the phone and rummage through every conceivable bit of data*, regardless of whether it bore any relevance whatsoever to the criminal activity at issue. Simply put, the warrant told the police to take everything, and they did. As such, the warrant was overbroad in every respect and violated the Fourth Amendment.

Id. at 922 (emphasis added); *see also Wey*, 256 F. Supp. 3d at 392 (quoting *Winn* for the proposition that "if [the applying officer] wants to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to [Defendant's] criminal activity, and he did not do so.") (quotation marks omitted). As a result, the court suppressed all evidence seized pursuant to the search warrant. *Winn*, 79 F. Supp. 3d at 926-27 (explaining that the warrant was a general warrant because "[e]very portion is impossibly overbroad, encompassing every conceivable bit of data generated by the use of the

cell phone at any point in time" and that "'the only remedy for a general warrant is to suppress all evidence obtained thereby.'") (quoting *United States v. Yusuf*, 461 F.3d 374, 393 (3d Cir. 2006)).

Similarly, in *In re Nextel Cellular Telephone*, law enforcement submitted an application for a warrant to search the contents of a cell phone seized incident to an arrest for drug trafficking. No. 14 MJ 8005, 2014 WL 2898262, at *1-2 (D. Kan. June 26, 2014). Like the Warrants here, the application sought to conduct a "full and complete forensic telephone examination" of the cell phone.[2] *Id*. at *2. The court denied the application as patently overbroad, noting in particular that the search methodology "will result in the overseizure of data and indefinite storage of data that it lacks probable cause to seize" and that it was "so broad that it appears to be nothing more than a 'general, exploratory rummaging in a person's belongings.'" *Id*. at *10 (*quoting Coolidge* 403 U.S. at 467). "Put another way", the court explained, "'[j]ust as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom,' probable cause to believe drug trafficking communication may be found in [a] phone's [] mail application will not support the search of the phone's Angry Birds application." *Id*. at *13 (*quoting United States v. Ross*, 456 U.S. 798, 824 (1982)).

To the extent that this Court concludes that the Warrants established probable cause to seize and search Defendants' phones in any manner, the search of those phones should have been limited to the locations on the phones where, according to the Applications, there was

[2] The search methodology at issue in *Nextel* included: "searching for and attempting to recover any deleted, hidden, or encrypted data . . . surveying various file directories and the individual files they contain; opening files in order to determine their contents; scanning storage areas; [and] performing keyword searches through all electronic storage areas[.]" *Id*.

probable cause to conclude evidence of criminality would be found. Even assuming—as two of the Applications assert—that cell phones used to communicate with others about fraud schemes "often contain records of that activity," those "records" here would be, at best, records of phone calls and a single text message. The Warrants, however, contained no limitation on the scope of the authorized searches. As in *Winn*, the Warrants authorized the Government to conduct "a complete review of the seized [electronically stored information]," which "may require *examination of all of the seized data* to evaluate its contents and determine whether the data is responsive to the warrant." (*See* Ex. 4 at JG_00000048; Ex. 5 at MC_00000115; Ex. 6 at CD_00000184) (emphasis added). Furthermore, the search methodology permitted by the Warrants is indistinguishable from the methodology that the court rejected as patently overbroad in *Nextel*, allowing law enforcement personnel to rummage through the entirety of the data contained on Defendants' phones to fish for evidence.

The Warrants contained no limitation whatsoever on the categories of data on Defendants' phones that the Government could search. Instead, the Warrants essentially "told the police to take everything, and they did." *Winn*, 79 F. Supp. 3d at 922. Because the Search Warrants permitted the Government to "rummage through every conceivable bit of data" contained on Defendants' cell phones, *Winn*, 79 F. Supp. 3d at 922, they were, "in function if not in form," general warrants. *Wey*, 256 F. Supp. 3d at 386. The Warrants were thus overbroad and violated the Fourth Amendment.

III. ALL EVIDENCE DERIVED FROM THE UNLAWFUL SEARCH OF DEFENDANTS' CELL PHONES MUST BE SUPPRESSED.

Because the Government lacked probable cause to search the entirety of the data contained on Defendants' cell phones, the Warrants were facially overbroad, and any law enforcement officer's reliance upon them was unreasonable. *See Leon*, 468 U.S. at 923, 104 S.

Ct. at 2134 (suppression is appropriate where a warrant is "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable."). Thus, the Government cannot carry its burden to "demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant," *George*, 975 F.2d at 77, and all evidence obtained from the searches of Defendants' phones must be suppressed.[3] *See Wey*, 256 F. Supp. 3d at 410-11 (suppressing all evidence obtained from overbroad warrant); *Winn*, 79 F. Supp. 3d at 926-27 (same).

IV. THE PRODUCT OF ANY SEARCH OF MR. GATTO'S CELL PHONE MUST ALSO BE SUPPRESSED BECAUSE THE PHONE WAS SEARCHED USING THE FRUITS OF A CUSTODIAL INTERROGATION IN VIOLATION OF HIS RIGHT TO COUNSEL.

The Government has represented to Mr. Gatto's counsel that FBI agents used Mr. Gatto's passcode to search his phone after the Government obtained the warrant to do so. The agents obtained Mr. Gatto's passcode in violation his right to counsel, and therefore the results of that search must be suppressed. *See Miranda v. Arizona,* 384 U.S. 436, 472-75, 86 S. Ct. 1602, 1626-28 (1966).

---

[3] Messrs. Code and Dawkins have standing to move for suppression because they maintain a reasonable expectation of privacy in their cell phones. *See Mancusi v. DeForte*, 392 U.S. 364, 369, 88 S. Ct. 2120, 2124 (1968); *United States v. Herron*, 2 F. Supp. 3d 391, 401 (E.D.N.Y. 2014) (defendant had a reasonable expectation of privacy in a cell phone because he was its "sole user"); Ex. 7 (Code Affidavit); Ex. 8 (Dawkins Affidavit). With respect to Mr. Gatto, although the Government's Warrant Application suggests that his iPhone is the property of his employer, adidas, *see* Ex. 1 at JG_00000006 n.1, the phone was purchased by Mr. Gatto for his exclusive use. *See United States v. Chuang*, 897 F.2d 646, 649 (2d Cir. 1990) (an employee has a reasonable expectation of privacy in his workplace and in employer-provided devices when "he has made a sufficient showing of a possessory or proprietary interest in the area searched."); *United States v. Tranquillo*, 606 F. Supp. 2d 370, 377 (S.D.N.Y. 2009) ("Generally, courts tend to find that these elements are sufficiently established when the area searched is set aside for the defendant's exclusive use[.]") (*quoting United States v. Hamdan*, 891 F. Supp. 88, 94-95 (E.D.N.Y. 1995)); Ex. 9 (Gatto Declaration). Therefore, Mr. Gatto has standing to make the instant motion.

After Mr. Gatto was placed under arrest at his home on September 26, 2017, he was informed of his *Miranda* rights by FBI agents and invoked his right to counsel. (Ex. 9 at ¶10.) Mr. Gatto then asked his wife to retrieve his iPhone so that he could place a call to counsel for his employer, adidas. An agent used Mr. Gatto's phone to speak with adidas' counsel, and did not return it. (*Id*.) Later, while he was handcuffed and in custody at the FBI's office, Mr. Gatto's phone—which was still in the possession of the FBI—began to ring, and an agent asked Mr. Gatto what the passcode was for the phone. In response to the agent's question, Mr. Gatto disclosed the passcode.[4] (*Id*.; Ex. 1 at JG_00000007 n.3.) Mr. Gatto was never asked for and did not provide consent to search his phone using the passcode. (Ex. 9 at ¶10.)

A. The Government Obtained Mr. Gatto's Passcode As a Result of Custodial Interrogation After He Invoked His Right To Counsel.

Mr. Gatto's statement to the FBI in which he provided the passcode to his iPhone was the product of custodial interrogation that occurred after Mr. Gatto was advised of his *Miranda* rights and invoked his right to counsel. When an individual is in custody, questioning from law enforcement is "inherently coercive" and *Miranda* and its progeny protects an individual's right to be free from such coercive interrogation. *United States v. Anderson*, 929 F.2d 96, 98 (2d. Cir. 1991) (noting that "in-custody interrogation contains psychological pressures that cause a suspect to speak when he would otherwise remain silent."). "If the individual states that he wants an attorney, the interrogation must cease until an attorney is present." *Miranda*, 384 U.S. at 474, 86 S. Ct. at 1628. Once *Miranda* rights have been invoked,

[4] In its application to search Mr. Gatto's phone, the Government asserted that at this time, an agent had previously observed Mr. Gatto's wife entering the passcode into Mr. Gatto's phone. (Ex. 1 at JG_00000007 n.3.) If, however, the agent already knew Mr. Gatto's passcode based on this observation, he would not have subsequently needed to ask Mr. Gatto for it.

that invocation must be "'scrupulously honored.'" *Anderson v. Smith*, 751 F.2d 96, 102 (2d Cir. 1984) (*quoting Michigan v. Mosley*, 423 U.S. 96, 104 (1975)).

While handcuffed and in custody at the FBI offices, an agent directly asked Mr. Gatto to provide him the passcode for Mr. Gatto's phone. Given the inherently coercive nature of questioning someone in custody, the FBI agent's question seeking Mr. Gatto's passcode constituted "express questioning or its equivalent" under the Supreme Court's definition, and Mr. Gatto's response constituted a testimonial communication. *See, e.g.*, *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1349 (11th Cir. 2012) ("The Fifth Amendment protects [the grand jury witness's] refusal to decrypt and produce the contents of the media devices because the act of decryption and production would be testimonial."); *United States v. Rogozin*, No. 09-CR-379, 2010 WL 4628520, at *6 (W.D.N.Y. Nov. 16, 2010) (suppressing incriminating statements made during border search without *Miranda* warnings, including a statement as to the passcode to an electronic device); *United States v. Kirschner*, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010) (government's post-indictment grand jury subpoena ordering defendant to provide all passcodes associated with his computer required defendant to make a "testimonial communication," and thus the subpoena violated defendant's Fifth Amendment privilege against compelled self-incrimination).

B. Data From Mr. Gatto's Cell Phone Should Be Suppressed As Fruit Of The Poisonous Tree.

Because the Government could not have obtained any information from the search of Mr. Gatto's iPhone but for the passcode that the agents procured from Mr. Gatto in violation of his *Miranda* rights, all data obtained from Mr. Gatto's iPhone must be suppressed as fruit of the poisonous tree. A recent opinion from the Eastern District of New York makes this point plain. In *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), federal law

enforcement stopped the defendant for questioning as he was boarding a flight to London because a cooperator had informed the Government that the defendant was involved in drug-smuggling. *Id*. at 298-99. Two federal agents searched the defendant's bags for currency and found multiple cell phones. *Id*. at 299. A third federal agent asked the defendant for the passcode to an iPhone, which the defendant provided. *Id*. at 299-300. Law enforcement then arrested and *Mirandized* the defendant, and ceased questioning him. *Id*. However, the Government used a Cellebrite device to extract 921 pages of data from the iPhone, which the Government called a "peek" at the device's contents. *Id*. at 307. The Government subsequently obtained a search warrant for the phone thirty days after the arrest, and claimed that in so doing, it did not rely on the initial "peek" at the cell phone. *Id*. at 303. The defendant moved to suppress all of the evidence seized from his phone, arguing that the evidence the Government obtained pursuant to the search warrant was the fruit of the initial warrantless search. *Id*. at 307. The court agreed with the defendant, and suppressed all evidence seized from his cell phone. *Id*. at 310. In so holding, the district court specifically rejected the Government's argument that it "would have inevitably been able to hack the phone" to get its contents if it didn't have the defendant's passcode, noting that the Government's proposed method to hack an iPhone (an IP-BOX) was unreliable and might actually destroy the data it sought. *See id*. at 310-11 (*citing In Re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, 15 MC 1902, (E.D.N.Y. Oct. 28, 2015)).

Because the Government accessed Mr. Gatto's cell phone using the passcode that it obtained as a result of violating his right to counsel, the information and data that it obtained as a result of its search pursuant to the Gatto Warrant must be suppressed.

V. DEFENDANTS' CELL PHONES AND THE IMAGED DATA OBTAINED FROM THOSE CELL PHONES MUST BE RETURNED TO DEFENDANTS.

Although the Second Circuit permits the use of mirror imaging to allow the Government to execute the search of the electronic data, *see Ganias*, 824 F.3d at 215, the Fourth Amendment requires the Government to execute the warrant by completing its review of that electronic data within a reasonable amount of time. *See, e.g., United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012). As the Second Circuit has acknowledged, the seizure and retention of electronic data "can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." *Ganias*, 824 F.3d at 217; *see also Doane v. United States*, No. 08–Mag.–17 (HBP), 2009 WL 1619642, at *10 (S.D.N.Y. June 5, 2009) (holding that when the government seizes documents, the Second Circuit's prior decisions "do not contemplate the indefinite retention of all materials contained within intermingled files.").

The Government is obligated to return any seized property that is beyond the scope of the warrant. "If the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular . . . data would become, in essence, a general warrant." *Ganias*, (2d Cir. 2014) *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016); *see also Doane*, 2009 WL 1619642, at *10 ("Thus, even where practical considerations permit the Government to seize items that are beyond the scope of the warrant, once the fruits of the search are segregated into responsive and non-responsive groups, the 'normal' practice is to return the non-responsive items."); *United States v Debbi*, 244 F. Supp. 2d 235, 237-39 (S.D.N.Y. 2003) (requiring the

government to return documents seized from defendant's residence that were beyond the scope of the warrant).

With respect to Messrs. Gatto and Dawkins—for whom Warrants were issued on October 10 and October 6, 2017, respectively—the Government has had approximately four months to search the imaged copies of their cell phones. The Code Warrant was issued on November 3, 2017, meaning that the Government has had over three months to complete its search of Mr. Code's phone. The Government has identified, and produced to Defendants, materials that it believes fall within the scope of the Warrants issued with respect to Messrs. Gatto and Dawkins. To the extent the Court concludes that any search of Defendants' cell phones was appropriate, the Government has had sufficient time to conduct that search and must now return all data that does not fall within the scope of the Warrants.

CONCLUSION

Accordingly, this Court should suppress the evidence obtained from the searches of Defendants' cell phones and order the Government to immediately return Defendants' cell phones, as well as the imaged copies of the cell phone data it maintains, to Defendants.

Dated: New York, New York
February 9, 2018

NEXSEN PRUET LLC

By: /s/ William W. Willkins
William W. Wilkins
Mark C. Moore
Andrew A. Mathias
55 E. Camperdown Way, Suite 400
Greenville, South Carolina 29601
(864) 370-2211
Attorneys for Defendant Merl Code

HANEY LAW GROUP PLLC

By: /s/ Steven A. Haney
Steven A. Haney
3000 Town Center Drive, Suite 2570
Southfield, Michigan 48075
(248) 414-1470
Attorneys for Defendant Christian Dawkins

WILLKIE FARR & GALLAGHER LLP

By: /s/ Michael S. Schachter
Michael S. Schachter
Casey E. Donnelly
787 Seventh Avenue
New York, New York 10019
(212) 728-8000

ANGELI LAW GROUP LLC
David Angeli
121 SW Morrison Street, Suite 400
Portland, Oregon 97204
(503) 222-1552
Attorneys for Defendant James Gatto